



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/242,210	11/04/1999	LINDA V GRAVELL	E-731	9775

7590 08/25/2004

CHARLES R MALANDRA JR  
PITNEY BOWES INC  
INTELLECTUAL PROPERTY AND TECHNOLOGY LAW DEP  
35 WATERVIEW DRIVE PO BOX 3000  
SHELTON, CT 06484

EXAMINER

SHERR, CRISTINA O

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

---

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
P.O. Box 1450  
ALEXANDRIA, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

MAILED  
AUG 25 2004  
GROUP 3000

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 09/242,210  
Filing Date: November 04, 1999  
Appellant(s): GRAVELL ET AL.

---

Brian A. Lemm  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 20 May 2004.

**(1) *Real Party in Interest***

A statement identifying the real party in interest is contained in the brief.

**(2) *Related Appeals and Interferences***

A statement identifying the related appeals and interferences that will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

**(3) *Status of Claims***

The statement of the status of the claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

Claims 2-8 have been canceled.

The statement of the status of claims 1 and 9-18 contained in the brief is correct.

**(4) *Status of Amendments After Final***

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) *Summary of Invention***

The summary of invention contained in the brief is correct.

**(6) *Issues***

The appellant's statement of the issues in the brief is correct.

**(7) Grouping of Claims**

The appellant's statement in the brief that certain claims do not stand or fall together is not agreed with because of the manner in which they are separately argued in the Appeal Brief. Claims 1 and 9-18 in this case are properly grouped as follows:

Group I - Claim 1.

Group II - Claims 9 and 12-13.

Group III - Claims 10-11.

Group IV - Claims 14 and 17-18.

Group V - Claims 15-16.

**(8) Claims Appealed**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(9) Prior Art of Record**

5,822,739	Kara	10-1998
6,005,945	Whitehouse	12-1999

**(10) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Kara (US 09/5,822,739).

Kara discloses a method for evidencing postage on a mail piece comprising the steps of receiving at a data center postal information relating to a mail piece, said postal information including recipient address information for the mail piece (col. 6, lines 34-38; col. 8, lines 24-29); generating a digital token for the mail piece, said digital token

including encrypted information for the mail piece based on said recipient address information (col. 8, lines 24-29; col. 14, lines 25-67); creating a transaction record, said transaction record including the digital the token and the postal information (col. 14, lines 29-36); signing the transaction record (col. 14, lines 30-36; a transaction record having "a unique transaction identifier"); storing the transaction record in a database (col. 14, lines 12-24); and performing value added services using the transaction record (col. 14, lines 39-41).

Claims 9-18 are rejected under 35 U.S.C. 102(e) as anticipated by Whitehouse (US 09/6,005,945).

Whitehouse discloses a system and method comprising a data center (102) communicatively coupled to a remote computer (104) via a network (e.g., Internet), a user initiating a request to the data center via the remote processor (110) to dispense postage value to be printed by a printer (108) coupled to the remote processor (110), the data center comprising a storage device (174) to store the user accounts (col. 8, lines 56-57) or meter accounts, and a first cryptographic module (161) coupled to the storage device (col. 12, lines 57-64) to verify the digital signature of the user.

Whitehouse further discloses a second cryptographic module (164) coupled to the storage device including keys to generate a digital token (col. 8, lines 38-41 or col. 11, lines 27-29), a key to decrypt a token key included in the meter account (col. 9, lines 35-39), a transaction record (e.g., amount of transaction) and a user transaction record (e.g., second transaction table record), coordinating encryption/decryption to keep the integrity of the balance update transaction (col. 14, lines 25-28, lines 43-46), the data

center sends the digital token to the remote processor via the Internet, a key management system (col. 18, line 41), on-line rating (col. 24, lines 1-11), and on-line tracking of all postal transaction processed by the data center (col. 8, lines 59-62).

Claims 9-18 are further rejected under 35 U.S.C. 103(a) as being unpatentable over Whitehouse (US 09/6,005,945).

Whitehouse does not explicitly disclose the use and locations of the first, second, third and fourth keys. However, Whitehouse clearly states the use of a key encryption method to secure the transactions and it would have been obvious to employ any number of keys as needed depending on the steps that the protection is desired, since it has been held that mere duplication of the essential working parts of a device involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ 8. Further, it would have been obvious to one having ordinary skill in the art at the time the invention was made to locate keys at any desirable modules, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse*, 86 USPQ 70.

## **(11) Response to Arguments**

### First issue

Appellant argues that Kara does not anticipate the subject matter defined by claim 1.

Specifically, Appellant contends that Kara does not disclose creating a transaction record, signing said transaction record, and storing said transaction record in a database. Kara, however, does disclose creating a transaction record (col. 14,

lines 29-36), signing the transaction record (col. 14, lines 30-36; a transaction record having "a unique transaction identifier"), as well as storing the transaction record in a database (col. 14, lines 12-24).

Appellant further argues that a digital signature authenticates and protects the integrity of the information in the transaction record. Nothing in claim 1, however, indicates such a protective function in the digital signature. Claim 1 does not even recite a digital signature *per se*. What is claimed is a "digital token." Additionally, Kara does disclose a fraud protection function as well as discussing the storage of transaction records in light of fraud protection at column 12, lines 15-25.

Appellant argues that nothing in Kara is related to creating a transaction record. Kara, however, discloses the generating or creating "a data packet" which "may include the date of posting, the amount of the postage, a unique transaction identifier . . . sender's return address, at the user's preference." (Col 14 ln 30-38). This data packet contains the information typically seen in any transaction record and is not limited to specific data listed in the paragraph. As such, Appellant argues features that are not expressly recited in the claims.

Thus, creating a transaction record, signing said transaction record, and storing said transaction record in a database is all disclosed in Kara.

#### Second issue

Appellant argues that the subject matter defined in claims 9-18 is not anticipated nor rendered obvious by Whitehouse.

With respect to claim 9, Appellant contends that nothing in Whitehouse discloses, teaches or suggests signing a transaction record associated with generating a digital token and storing the signed transaction record in the storage device of the data center as recited in claim 9.

Whitehouse does, however, disclose signing a transaction record in association with generating a digital token (col. 8, lines 38-41 or col. 11, lines 27-29), coupled to a storage device where said transaction is stored (col 11 ln 30-35). Specifically, Whitehouse refers to a “[p]ublic key reference number (indicating which key was used by the central computer to digitally sign the postage indicium for this postage dispensing event).” (col 11 ln 26-29). Whitehouse then goes on to explain that it is this transaction file that “will require the largest amount of data storage on the central computer.” (col 11 ln 30-31). Thus, Whitehouse does disclose signing a transaction record associated with generating a digital token and storing the signed transaction record in the storage device of the data center.

Appellant further argues, with respect to claim 9 that the rejection uses impermissible hindsight to reconstruct the present invention from the Whitehouse reference. However, Whitehouse clearly states the use of a key encryption method to secure the transactions and it would have been obvious to employ any number of keys as needed depending on the steps that the protection is desired, since it has been held that mere duplication of the essential working parts of a device involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ 8. Further, it would have been obvious to one having ordinary skill in the art at the time the invention was made to



locate keys at any desirable modules, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse*, 86 USPQ 70.

With respect to claim 10, Appellant argues that nothing in White house teaches or suggests a third cryptographic module coupled to the storage device, where the third module includes a fourth key used to sign a user transaction record which is stored in the storage device. Whitehouse does not explicitly disclose the use and locations of the first, second, third and fourth keys. However, Whitehouse clearly states the use of a key encryption method to secure the transactions and it would have been obvious to employ any number of keys as needed depending on the steps that the protection is desired, since it has been held that mere duplication of the essential working parts of a device involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ 8. Further, it would have been obvious to one having ordinary skill in the art at the time the invention was made to locate keys at any desirable modules, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse*, 86 USPQ 70.

With respect to claim 14, Appellant contends that nothing in Whitehouse discloses, teaches or suggests signing a transaction record associated with generating a digital token and storing the signed transaction record in the storage device of the data center as recited in claim 14.

Whitehouse does, however, disclose signing a transaction record in association with generating a digital token (col. 8, lines 38-41 or col. 11, lines 27-29), coupled to a storage device where said transaction is stored (col 11 In 30-35). Specifically,

Whitehouse refers to a “[p]ublic key reference number (indicating which key was used by the central computer to digitally sign the postage indicium for this postage dispensing event).” (col 11 ln 26-29). Whitehouse then goes on to explain that it is this transaction file that “will require the largest amount of data storage on the central computer.” (col 11 ln 30-31). Thus, Whitehouse does disclose signing a transaction record associated with generating a digital token and storing the signed transaction record in the storage device of the data center.

With respect to claim 15, Appellant argues that nothing in Whitehouse appears to teach or suggest using a fourth key to sign a user transaction record that is stored at the data center as is recited in claim 15.

Whitehouse does not explicitly disclose the use and locations of the first, second, third and fourth keys. However, Whitehouse clearly states the use of a key encryption method to secure the transactions and it would have been obvious to employ any number of keys as needed depending on the steps that the protection is desired, since it has been held that mere duplication of the essential working parts of a device involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ 8. Further, it would have been obvious to one having ordinary skill in the art at the time the invention was made to locate keys at any desirable modules, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse*, 86 USPQ 70.

For the above reasons, it is believed that the rejections should be sustained.



August 10, 2004

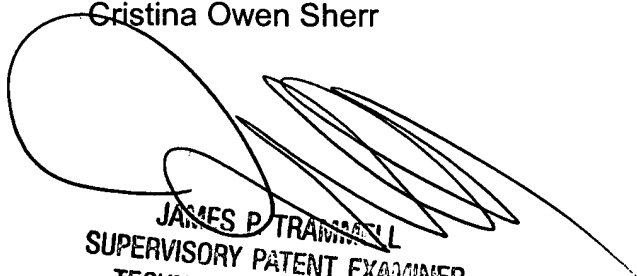
Conferees

James Trammel

  
Joseph Thomas

Respectfully submitted,

Cristina Owen Sherr



JAMES P. TRAMMELL  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3300

BRIAN A. LEMM

CHARLES R MALANDRA JR  
PITNEY BOWES INC  
INTELLECTUAL PROPERTY AND TECHNOLOGY LAW DEP  
35 WATERVIEW DRIVE PO BOX 3000  
SHELTON, CT 06484